Welcome to the PIA for FY 2011!

Congress passed the E-Government Act of 2002 to encourage the use of Web-based Internet applications or other information technology by Government agencies, with the intention of enhancing access to government information and services and increasing the effectiveness, efficiency, and quality of government operations.

To combat public concerns regarding the disclosure of private information, the E-Government Act mandated various measures, including the requirement that Federal agencies conduct a Privacy Impact Assessment (PIA) for projects with information technology systems that collect, maintain, and/or disseminate "personally identifiable information" of the public. Personally identifiable information, or "personal information," is information that may be used to identify a specific person.

The Privacy Act and VA policy require that personally identifiable information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

Directions:
VA 6508 is the directive which outlines the PIA requirement for every System/Application/Program.

If you find that you can't click on checkboxes, make sure that you are: 1) Not in "design mode" and 2) you have enabled macros.

PIA Website: http://vaww.privacy.va.gov/Privacy_Impact_Assessments.asp

Roles and Responsibilities:
Roles and responsibilities for the specific process are clearly defined for all levels of staff in the VA Directive 6508 referenced in the procedure section of this document.

a. The Privacy Officer is responsible for the overall coordination and review of the PIA to ensure compliance with VA Directive 6508.

b. Records Officer is responsible for supplying records retention and deletion schedules.

c. Information Technology (IT) staff responsible for the privacy of the system data will perform a PIA in accordance with VA Directive 6508 and to immediately report all anomalies to the Privacy Service and appropriate management chain.

d. Information Security Officer (ISO) is responsible for assisting the Privacy Officer and providing information regarding security controls.

e. The CIO is responsible for ensuring that the systems under his or her jurisdiction undergo a PIA. This responsibility includes identifying the IT systems; coordinating with the Privacy Officer, Information Security Officer, and others who have concerns about privacy and security issues; and reviewing and approving the PIA before submission to the Privacy Service.

Definition of PII (Personally Identifiable Information)
Information in identifiable form that is collected and stored in the system that either directly identifies and individual by name, address, social security number, telephone number, e-mail address, biometric identifiers, photograph, or other unique numbers, codes or characteristics or combined, indirect indentify an individual such as a combination of gender, race, birth date, geographical indicators, license number is also considered PII.

Macros Must Be Enabled on This Form
Microsoft Office 2003: To enable macros, go to: 1) Tools > Macros > Security - Set to Medium; 2) Click OK; 3) Close the file and when reopening click on Enable Macros at the prompt.

Microsoft Office 2007: To enable macros, go to: 1) Office Button > Prepare > Excel Options > Trust Center > Trust Center Settings > Macro Settings > Enable

All Macros; 2) Click OK

Final Signatures

Final Signatures are digitally signed or wet signatures on a case by case basis. All signatures should be done when all modifications have been approved by the VA Privacy Service and the reviewer has indicated that the signature is all that is necessary to obtain approval.

Privacy Impact Assessment Uploaded into SMART

Privacy Impact Assessments should be uploaded into C&A section of SMART.

All PIA Validation Letters should be emailed to christina.pettit@va.gov to received full credit for submission.

(FY 2011) PIA: System Identification

Program or System Name:	Region 3-Detroit VAMC 553-LAN
OMB Unique System / Application / Program Identifier (AKA: UPID #):	029-00-02-00-01-1120-00

Description of System/ Application/ Program:

Each VA medical center uses the Local Area Network (LAN) as a General Support System, supporting mission-critical and other systems necessary to conduct day-to-day operations within the Veterans Health Administration. Applications and devices within the LAN support numerous areas, including medical imaging, supply management, decision support, medical research, and education.

Facility Name:	John D. Dingell VA Medical System		
Title:	**Name:**	**Phone:**	**Email:**
Privacy Officer:	Michele Rickard	313-576-3680	michele.rickard@va.gov
Information Security Officer:	Jocelyn Gateley	313-576-1000 ext 65235	jocelyn.gateley@va.gov
System Owner/ Chief Information Officer:	Jonathan Small	313-576-1000 ext 65169	jonathan.small@va.gov
Site Manager	Mark E. Russell	313-576-3776	markie.russell@va.gov
Other Titles: Alternate Privacy Officer	Margaret Ekaiko-Davis	313-576-1000 ext. 63370	margaret.ekaiko-davis@va.gov
Person Completing Document:	Michele Rickard	313-576-3680	michele.rickard@va.gov
Other Titles: Secondary Information Security Officer	Henry Foutner	313-576-3875	henry.foutner@va.gov

Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)	08/2008
Date Approval To Operate Expires:	04/2011
What specific legal authorities authorize this program or system:	Title 38, United States Code, section 7301(a).
What is the expected number of individuals that will have their PII stored in this system:	approximately 1,000,000
Identify what stage the System / Application / Program is at:	Operations/Maintenance
The approximate date (MM/YYYY) the system will be operational (if in the Design or Development stage), or the approximate number of years the system/application/program has been in operation.	Approximately 30+ years, 1979 to present
Is there an authorized change control process which documents any changes to existing applications or systems?	Yes
If No, please explain:	
Has a PIA been completed within the last three years?	No
Date of Report (MM/YYYY):	03/2011

Please check the appropriate boxes and continue to the next TAB and complete the remaining questions on this form.

☐ Have any changes been made to the system since the last PIA?

☑ Is this a PIV system/application/program collecting PII data from Federal employees, contractors, or others performing work for the VA?

☑ Will this system/application/program retrieve information on the basis of name, unique identifier, symbol, or other PII data?

☑ Does this system/application/program collect, store or disseminate PII/PHI data?

☑ Does this system/application/program collect, store or disseminate the SSN?

If there is no Personally Identifiable Information on your system , please complete TAB 7 & TAB 12. (See Comment for Definition of PII)

2. System Identification

(FY 2011) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records? If the answer above no, please skip to row 15.	Yes
For each applicable System(s) of Records, list:	
1. All System of Record Identifier(s) (number):	24VA19
2. Name of the System of Records:	Patient Medical Records
3. Location where the specific applicable System of Records Notice may be accessed (include the URL):	http://vaww.vhaco.va.gov/privacy/Systemofecords.htm
Have you read, and will the application, system, or program comply with, all data management practices in the System of Records Notice(s)?	Yes
Does the System of Records Notice require modification or updating?	No
	(Please Select Yes/No)
Is PII collected by paper methods?	Yes
Is PII collected by verbal methods?	Yes
Is PII collected by automated methods?	No
Is a Privacy notice provided?	Yes
Proximity and Timing: Is the privacy notice provided at the time of data collection?	Yes
Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?	Yes
Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?	Yes
Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?	Yes

(FY 2011) PIA: Notice

Please fill in each column for the data types selected.

Data Type	Collection Method	What will the subjects be told about the information collection?	How is this message conveyed to them?	How is a privacy notice provided?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Verbal	The most common data types that are captured and accessed on a regular basis by authorized individuals are first and last name, middle initial, DOB, SSN, and address. This patient information falls into two classes: administrative and clinical. Clinical information is used to diagnose, prescribe treatment and follow clinically the patient through his/her health care encounters. Administrative data is used to identify the veteran (SSN), correspond to/from (name and address), and determine eligibility (patient administrative info + SSA and IRS data).	Verbally	Written
Family Relation (spouse, children, parents, grandparents, etc)	Paper	Dependent Data is utilized to determine eligibility for VA benefits. In addition, NOK and emergency contact information is often a dependent of the veteran and this data is used in case of emergency or need during the patient's episode of care.	Written	Written

Service Information	ALL	Military Service Information (Branch of service, discharge date, discharge type, service connection rating, medical conditions related to military service, etc). This information is collected to assess eligibility for VA healthcare benefits, type of healthcare needed.	Verbal & Written	Written
Medical Information	Verbal	VistA-Legacy applications and meet a wide range of health care data needs. The VistA-Legacy system operates in medical centers, ambulatory and community-based clinics, nursing homes and domiciliary, and thus collects a wide range of personal medical information for clinical diagnosis, treatment, patient evaluation, and patient care. Common types of personal medical information would include lab test results, prescriptions, allergies, medical diagnoses, vital signs, etc. The information is used to treat and care for the veteran patient. Clinical information from VA and DoD is used in the diagnosis and treatment of the veteran.	Verbally	Written

Criminal Record Information	Electronic/File Transfer	Specific information is not input into the VistA system but the fugitive felon program includes a flag on the patient file identifying the need to contact the VA police.	Verbally	Written
Guardian Information	Verbal	Guardian information is often flagged in the medical record to ensure the timely and appropriate notification during healthcare decision making from provider/patient/guardian.	Written	Written
Education Information	N/A			
Benefit Information	Electronic/File Transfer	VIS, HINQ, VERA, KLF, used to verify service dates, eligibility, SSN, etc.	Verbally	Written
Other (Explain)	Paper	Next-of-kin information and emergency contact information, such as name and telephone number, is collected from the veteran to use to contact other individuals in case of an emergency. In addition insurance and employment information is available on the veteran for use in billing for care. Religious information is collected to provide for spiritual needs if requested by the veteran.	Verbally	Written

Data Type	Is Data Type Stored on your system?	Source (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?	Additional Comments
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	Veteran	Mandatory	The intended use of this information is to appropriately identify the patient and accurately link patient records under VA systems as appropriate to provide for accurate clinical decision making and continuity of care. Beneficiaries sign 'Release of Information Waivers' which are kept on file. We reject claims that indiciate the ROI statement is not onfile. It is on the Application for Benefits.
Family Relation (spouse, children, parents, grandparents, etc)	Yes	Veteran	Mandatory	Next of Kin and Emergency Contact information; names, addresses, phone numbers. Used for notification in case of emergency.

Service Information				Military branch, rank, discharge information, and dates of service - as described on the official DD-214. Service Information for both benefits and Eligibility needs
	Yes	Veteran	Mandatory	
Medical Information				Diagnosis, medical history, current problem list, prescriptions, surgeries and family history All medical information is to provide care to veterans. The clinicians have the responsibility to distinguish between relevant and irrelevant information that relates to the care of the veteran.
	Yes	Veteran	Mandatory	
Criminal Record Information				Name, SSN, DOB, Address, Telephone numbers, Geographic location. Required by Federal statute to identify wanted felons.
	Yes	Veteran	Mandatory	

Guardian Information				Yes, where applicable. Guardian information on those veterans where necessary for identification and benefit disbursement, as well as medical decision-making factors.
	Yes	Veteran	Mandatory	
Education Information	Yes	Veteran	Voluntary	
Benefit Information				VIS, HINQ, VERA, KLF, used to verify service dates, eligibility, SSN, etc.
	Yes	VA Files / Databases (Identify file)		
Other (Explain)				
Other (Explain)				
Other (Explain)				

(FY 2011) PIA: Data Sharing

Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing and its purpose.	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization	VBA	No	treatment and demographic for benefits determination	PII	MCM-00-29, MCM 001B-69
Other Veteran Organization	Office of Regional Counsel	No	Tort Claims, legal processes	Both PII & PHI	BAA
Other Federal Government Agency	Congressional Offices, SSA, DoD	No	Appointment dates, treatment, medical documentation, bills, co-pays	Both PII & PHI	ROI - 001B-17, MCM 001B-69
State Government Agency	CDC	No	HIV and other infectious disease results	Both PII & PHI	DUA
Local Government Agency	N/A				
Research Entity	Karmanos/Wayne State University	No	Tumor Registry	Both PII & PHI	DUA/MOU
Other Project / System					
Other Project / System					
Other Project / System					

(FY 2011) PIA: Access to Records

Does the system gather information from another system?	No
Please enter the name of the system:	
Per responses in Tab 4, does the system gather information from an individual?	Yes

If information is gathered from an individual, is the information provided:
- ☑ Through a Written Request
- ☑ Submitted in Person
- ☐ Online via Electronic Form

Is there a contingency plan in place to pro

(FY 2011) PIA: Secondary Use

Will PII data be included with any secondary use request?   No

if yes, please check all that apply:
☐ Drug/Alcohol Counseling   ☐ Mental Health   ☐ HIV
☐ Research   ☐ Sickle Cell   ☐ Other (Please Explain)

Describe process for authorizing access to this data.

Answer: when needed a signed authorization, DUA, MOU must be in place prior to release of any information

(FY 2011) PIA: Program Level Questions

Does this PIA form contain any sensitive information that could cause harm to the Department of Veterans Affairs or any party if disclosed to the public?　　No

If Yes, Please Specify:

Explain how collected data are limited to required elements:
Answer: Data is collected and entered to the appropriate application by staff who have been assigned a specific functional category

How is data checked for completeness?
Answer: Services are responsible to conduct monitors and audits as outlined by JC, PCA, ITOC etc.

What steps or procedures are taken to ensure the data remains current and not out of date?
Answer: Patient information is updated and/or verified at each visit. Periodic reports are also run to insure accuracy and info is up to date.

How is new data verified for relevance, authenticity and accuracy?
Answer: New data is verified through patient verification and compared against other (paper) sources

Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)
Answer:

(FY 2011) PIA: Retention & Disposal

What is the data retention period?
Answer: 75 years after the last episode of care.

Explain why the information is needed for the indicated retention period?
Answer: Clinical information is retained in accordance with VA Records Control Schedule 10-1.

What are the procedures for eliminating data at the end of the retention period?
Answer: Electronic Final Version of Patient Medical Record is destroyed/deleted 75 years after the last episode of patient care as instructed in VA Records Control Schedule 10-1, Item XLIII, 2.b. (Page 190).

Where are these procedures documented?
Answer: Record Control Schedule 10-1

How are data retention procedures enforced?
Answer: Program officials are responsible for creating, maintaining. protecting, and disposing of records in their program area in accordance with NARA regulations and VA policy. All VHA employees are responsible to ensure that records are created, maintained, protected, and disposed of in accordance with NARA regulations and VA policies and procedures.

Has the retention schedule been approved by the National Archives and Records Administration (NARA)　　Yes

Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)
Answer:

(FY 2011) PIA: Children's Online Privacy Protection Act (COPPA)

Will information be collected through the internet from children under age 13?　　No

If Yes, How will parental or guardian approval be obtained?

Answer:

Is the system/application/program following IT security Requirements and procedures required by federal law and policy to ensure that information is appropriately secured.	Yes
Has the system/application/program conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls..	Yes

Is security monitoring conducted on at <u>least</u> a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	Yes
Is security testing conducted on at <u>least</u> a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	Yes
Are performance evaluations conducted on at <u>least</u> a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	Yes
If 'No' to any of the 3 questions above, please describe why:	
Answer:	

Is adequate physical security in place to protect against unauthorized access?	Yes
If 'No' please describe why:	
Answer:	

Explain how the project meets IT security requirements and procedures required by federal law.

Answer: The facility follows the Office of Cyber & Information Security (OCIS) established directives, policies, & procedures which are consistent with the provisions of Federal Information Security Management Act (FISMA) as well as guidance issued by the Office of Management & Budget (OMB), the National Institute of Standards & Technology (NIST), & other requirements that VistA-Legacy is and has been subject to. At the end of the life cycle of the project any data contained on hardware/equipment is mandated to be sanitized via the approved VA method.

Explain what security risks were identified in the security assessment? *(Check all that apply)*

☐ Air Conditioning Failure	☑ Data Disclosure	☑ Hardware Failure
☐ Chemical/Biological Contamination	☑ Data Integrity Loss	☑ Identity Theft
☐ Blackmail	☐ Denial of Service Attacks	☑ Malicious Code
☐ Bomb Threats	☐ Earthquakes	☑ Power Loss
☐ Burglary/Break In/Robbery	☐ Eavesdropping/Interception	☐ Sabotage/Terrorism
☐ Cold/Frost/Snow	☐ Errors (Configuration and Data Entry)	☑ Storms/Hurricanes
☑ Communications Loss	☑ Fire (False Alarm, Major, and Minor)	☐ Substance Abuse
☐ Computer Intrusion	☑ Flooding/Water Damage	☑ Theft of Assets
☑ Computer Misuse	☐ Fraud/Embezzlement	☑ Theft of Data
☑ Data Destruction		☑ Vandalism/Rioting

☑ Data Destruction   ☐ Fraud/Embezzlement   ☑ Vandalism/Rioting

Answer: (Other Risks)

Explain what security controls are being used to mitigate these risks. *(Check all that apply)*

☑ Access Control   ☑ Contingency Planning   ☑ Personnel Security

☑ Audit and Accountability   ☑ Identification and Authentication   ☑ Physical and Environmental Protection

☑ Awareness and Training   ☑ Incident Response

☑ Certification and Accreditation Security Assessments   ☑ Risk Management

☑ Configuration Management   ☑ Media Protection

Answer: (Other Controls)

PIA: PIA Assessment

Identify what choices were made regarding the project/system or collection of information as a result of performing the PIA.
Controls are in place to mitigate misuse of information, provide privacy notices along with security controls

<u>Availability Assessment:</u> If the data being collected is not available to process for any reason what will the potential impact be upon the system or organization? **(Choose One)**	☐ The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
	☐ The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.
	☑ The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.
<u>Integrity Assessment:</u> If the data being collected has been corrupted for any reason what will the potential impact be upon the system or organization? **(Choose One)**	☑ The potential impact is **high** if the loss of integrity could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
	☐ The potential impact is **moderate** if the loss of integrity could be expected to have a serious adverse effect on operations, assets or individuals.
	☐ The potential impact is **low** if the loss of integrity could be expected to have a limited adverse effect on operations, assets or individuals.
<u>Confidentiality Assessment:</u> If the data being collected has been shared with unauthorized individuals what will the potential impact be upon the system or organization? **(Choose One)**	☑ The potential impact is **high** if the loss of confidentiality could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
	☐ The potential impact is **moderate** if the loss of confidentiality could be expected to have a serious adverse effect on operations, assets or individuals.
	☐ The potential impact is **low** if the loss of confidentiality could be expected to have a limited

adverse effect on operations, assets or individuals.

The controls are being considered for the project based on the selections from the previous assessments?

The minimum security requirements for our high impact system cover seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives.

Please add additional controls:

(FY 2011) PIA: Additional Comments

Add any additional comments or information that may have been left out for any question. Please indicate the question you are responding to and then add your comments.

Which of these are sub-components of your system?

Access Manager	Automated Sales Reporting (ASR)	Automated Folder Processing System (AFPS)
Actuarial	BCMA Contingency Machines	Automated Medical Information Exchange II (AIME II)
Appraisal System	Benefits Delivery Network (BDN)	Automated Medical Information System (AMIS)290
ASSISTS	Centralized Property Tracking System	Automated Standardized Performace Elements Nationwide (ASPEN)
Awards	Common Security User Manager (CSUM)	Centralized Accounts Receivable System (CARS)
Awards	Compensation and Pension (C&P)	Committee on Waivers and Compromises (COWC)
Baker System	Control of Veterans Records (COVERS)	Compensation and Pension (C&P) Record Interchange (CAPRI)
Bbraun (CP Hemo)	Control of Veterans Records (COVERS)	Compensation & Pension Training Website
BDN Payment History	Control of Veterans Records (COVERS)	Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)
BIRLS	Courseware Delivery System (CDS)	Distribution of Operational Resources (DOOR)
C&P Payment System	Dental Records Manager	Educational Assistance for Members of the Selected Reserve Program CH 1606
C&P Training Website	Education Training Website	Electronic Performance Support System (EPSS)
CONDO PUD Builder	Electronic Appraisal System	Enterprise Wireless Messaging System (Blackberry)
Corporate Database	Electronic Card System (ECS)	Financial Management Information System (FMI)
Data Warehouse	Electronic Payroll Deduction (EPD)	Hearing Officer Letters and Reports System (HOLAR)
EndoSoft	Eligibility Verification Report (EVR)	Inquiry Routing Information System (IRIS)
FOCAS	Fiduciary Beneficiary System (FBS)	Modern Awards Process Development (MAP-D)
Inforce	Fiduciary STAR Case Review	Personnel and Accounting Integrated Data and Fee Basis (PAID)
INS - BIRLS	Financial and Accounting System (FAS)	Personal Computer Generated Letters (PCGL)
Insurance Online	Insurance Unclaimed Liabilities	Personnel Information Exchange System (PIES)
Insurance Self Service	Inventory Management System (IMS)	Personnel Information Exchange System (PIES)
LGY Home Loans	LGY Centralized Fax System	Post Vietnam Era educational Program (VEAP) CH 32
LGY Processing	Loan Service and Claims	Purchase Order Management System (POMS)
Mobilization	Loan Guaranty Training Website	Reinstatement Entitelment Program for Survivors (REAPS)
Montgomery GI Bill	Master Veterans Record (MVR)	Reserve Educational Assistance Program CH 1607
MUSE	Mental Health Asisstant	Service Member Records Tracking System
Omnicell	National Silent Monitoring (NSM)	Survivors and Dependents Education Assistance CH 35
Priv Plus	Powerscribe Dictation System	Systematic Technical Accuracy Review (STAR)
RAI/MDS	Rating Board Automation 2000 (RBA2000)	Training and Performance Support System (TPSS)
Right Now Web	Rating Board Automation 2000 (RBA2000)	VA Online Certification of Enrollment (VA-ONCE
SAHSHA	Rating Board Automation 2000 (RBA2000)	VA Reserve Educational Assistance Program
Script Pro	Records Locator System	Veterans Appeals Control and Locator System (VACOLS)
SHARE	Review of Quality (ROQ)	Veterans Assistance Discharge System (VADS)
SHARE	Search Participant Profile (SPP)	Veterans Exam Request Info System (VERIS)
SHARE	Spinal Bifida Program Ch 18	Veterans Service Representative (VSR) Advisor
Sidexis	State Benefits Reference System	Vocational Rehabilitation & Employment (VR&E) CH 31
Synquest	State of Case/Supplemental (SOC/SSOC)	Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)

VBA Data Warehouse	Telecare Record Manager	Web Automated Folder Processing System (WAFPS)
VBA Training Academy	VBA Enterprise Messaging System	Web Automated Reference Material System (WARMS)
Veterans Canteen Web	Veterans On-Line Applications (VONAPP)	Web Automated Verification of Enrollment
VIC	Veterans Service Network (VETSNET)	Web-Enabled Approval Management System (WEAMS)
VR&E Training Website	Web Electronic Lender Identification	Web Service Medical Records (WebSMR)
Web LGY		Work Study Management System (WSMS)

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

Name Description Comments Is PII collected by this min or application? Does this minor application store PII? If yes, where? Who has access to this data?

Name Description Comments Is PII collected by this min or application? Does this minor application store PII? If yes, where? Who has access to this data?

Name Description Comments Is PII collected by this min or application? Does this minor application store PII? If yes, where? Who has access to this data?

Which of these are sub-components of your system?

ASISTS	Beneficiary Travel	Accounts Receivable	Adverse Reaction Tracking
Bed Control	Care Management	ADP Planning (PlanMan)	Authorization/ Subscription
CAPRI	Care Tracker	Bad Code Med Admin	Auto Replenishment/ Ward Stock
CMOP	Clinical Reminders	Clinical Case Registries	Automated Info Collection Sys
Dental	CPT/ HCPCS Codes	Clinical Procedures	Automated Lab Instruments
Dietetics	DRG Grouper	Consult/ Request Tracking	Automated Med Info Exchange
Fee Basis	DSS Extracts	Controlled Substances	Capacity Management - RUM
GRECC	Education Tracking	Credentials Tracking	Capacity Management Tools
HINQ	Engineering	Discharge Summary	Clinical Info Resource Network
IFCAP	Event Capture	Drug Accountability	Clinical Monitoring System
Imaging	Extensible Editor	EEO Complaint Tracking	Enrollment Application System
Kernal	Health Summary	Electronic Signature	Equipment/ Turn-in Request
Kids	Incident Reporting	Event Driven Reporting	Gen. Med.Rec. - Generator
Lab Service	Intake/ Output	External Peer Review	Health Data and Informatics
Letterman	Integrated Billing	Functional Independence	ICR - Immunology Case Registry
Library	Lexicon Utility	Gen. Med. Rec. - I/O	Income Verification Match
Mailman	List Manager	Gen. Med. Rec. - Vitals	Incomplete Records Tracking
Medicine	Mental Health	Generic Code Sheet	Interim Mangement Support
MICOM	MyHealthEVet	Health Level Seven	Master Patient Index VistA
NDBI	National Drug File	Hospital Based Home Care	Missing Patient Reg (Original) A4EL
NOIS	Nursing Service	Inpatient Medications	Order Entry/ Results Reporting
Oncology	Occurrence Screen	Integrated Patient Funds	PCE Patient Care Encounter
PAID	Patch Module	MCCR National Database	Pharmacy Benefits Mangement
Prosthetics	Patient Feedback	Minimal Patient Dataset	Pharmacy Data Management
QUASER	Police & Security	National Laboratory Test	Pharmacy National Database
RPC Broker	Problem List	Network Health Exchange	Pharmacy Prescription Practice
SAGG	Progress Notes	Outpatient Pharmacy	Quality Assurance Integration
Scheduling	Record Tracking	Patient Data Exchange	Quality Improvement Checklist
Social Work	Registration	Patient Representative	Radiology/ Nuclear Medicine
Surgery	Run Time Library	PCE Patient/ HIS Subset	Release of Information - DSSI
Toolkit	Survey Generator	Security Suite Utility Pack	Remote Order/ Entry System
Unwinder	Utilization Review	Shift Change Handoff Tool	Utility Management Rollup
VA Fileman	Visit Tracking	Spinal Cord Dysfunction	CA Vertified Components - DSSI
VBECS	VistALink Security	Text Integration Utilities	Vendor - Document Storage Sys
VDEF	Women's Health	VHS & RA Tracking System	Visual Impairment Service Team ANRV
VistALink		Voluntary Timekeeping	x Voluntary Timekeeping National

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

Name	Fee Basis Claims System (FBCS)?????
Description	
Comments	
Is PII collected by this minor application?	
Does this minor application store PII?	
If yes, where?	
Who has access to this data?	

Name	
Description	
Comments	
Is PII collected by this minor application?	
Does this minor application store PII?	
If yes, where?	
Who has access to this data?	

Name	
Description	
Comments	
Is PII collected by this minor application?	
Does this minor application store PII?	
If yes, where?	
Who has access to this data?	

Which of these are sub-components of your system?

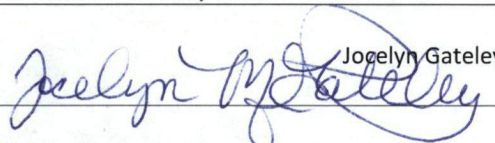|			
x	1184 Web	ENDSOFT	RAFT
		Enterprise Terminology Server &	RALS
	A4P	VHA Enterprise Terminology	
x		Services	

(FY 2011) PIA: Final Signatures

Facility Name: Region 3-Detroit VAMC 553-LAN

Title:	Name:	Phone:	Email:
Privacy Officer:	Michele Rickard	313-576-3680	michele.rickard@va.gov

Michele Rickard — Digitally signed by: Michele Rickard
DN: CN = Michele Rickard C = US
OU = Privacy/FOIA Officer
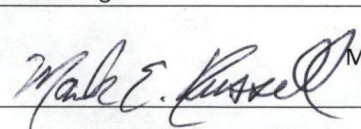Date: 2011.05.10 16:18:55 -05'00'   Michele Rickard

		313-576-1000 ext 65235	
Information Security Officer:	Jocelyn Gateley		jocelyn.gateley@va.gov

Jocelyn Gateley
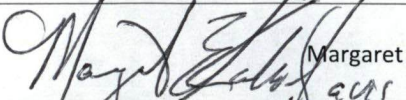
		313-576-1000 ext 65169	
System Owner/ Chief Information Officer:	Jonathan Small		jonathan.small@va.gov

JONATHAN E. SMALL 243159 — Digitally signed by JONATHAN E. SMALL 243159
DN: dc=gov, dc=va, o=internal, ou=people,
0.9.2342.19200300.100.1.1=jonathan.small@
va.gov, cn=JONATHAN E. SMALL 243159
Date: 2011.05.11 08:35:36 -04'00'   Jonathan Small

Site Manager	Mark E. Russell	313-576-3776	markie.russell@va.gov

Mark E. Russell

		313-576-1000 ext. 63370	
Other Titles: Alternate Privacy Officer	Margaret Ekaiko-Davis		margaret.ekaiko-davis@va.gov

Margaret Ekaiko-Davis

Date of Report: 3/3/11

OMB Unique Project Identifier   029-00-02-00-01-1120-00

                                Region 3 > VISN 11 > Detroit VAMC

Project Name   > LAN